UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,725	12/07/2005	Yuichi Futa	2005_1849A	1837

52349 7590 01/23/2009

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
KING, JOHN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
01/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/559,725	FUTA ET AL.	
	Examiner	Art Unit	
	JOHN B. KING	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14 and 15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14 and 15* is/are rejected.

7)☒ Claim(s) *7* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on October 28, 2008.

2. Claims 1-12 and 14-15 are pending in this application. Claims 13 and 16 are cancelled and Claims 11-12 and 14-15 are amended by applicant's amendment.

3. Applicant's arguments in respect to the new issues of claims 1-12 and 14-15 have been considered but they are not persuasive.

Examiner Notes

4. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Objections

5. Claim 7 is objected to because of the following informalities: The term "message" has been misspelled as "mesasage" in line 8 of the amended claim. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-2, 7-10 and 14-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamichi et al. (US 2002/0116612 A1) published August 22, 2002, hereinafter referred to as Yamamichi in view of Olson et al. (US Pre-Grant Publication 2003/0226007 A1) filled May 30, 2002 hereinafter referred to as Olson.

As per claim 1, Yamamichi discloses an encryption communication system for secret message communication, the encryption communication system comprising an encryption transmission apparatus and an encryption reception apparatus **(paragraph 27, Yamamichi teaches having a transmission apparatus and reception apparatus in order to encrypt data.)**, wherein the encryption transmission apparatus includes: a storage unit that stores one message **(paragraph 56, Yamamichi teaches having plaintext storage to store the message to be encrypted.)**; an encryption unit operable to perform an encryption computation on the one message a plural number of times **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple encrypted messages.)**, to generate a plurality of encrypted

messages from the one message **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n.)**, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**; a computation unit operable to perform a one-way operation on the one message to generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the plaintext message to calculate a value.)**; and a transmission unit operable to transmit **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple encrypted messages.)**, and wherein the encryption reception apparatus includes: a reception unit operable to receive **(paragraph 84, Yamamichi teaches**

having a receiving unit to receive the encrypted data.), from the encryption transmission apparatus **(paragraph 84, Yamamichi teaches the receiving unit receiving data from the transmission apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted message and the hash value from the transmission apparatus. Yamamichi, paragraph 14, also teaches the reception of the multiple encrypted messages.)**; a decryption unit operable to perform a decryption computation **(paragraphs 85- 90, Yamamichi teaches having a decrypting unit to decrypt the encrypted data.)**, corresponding to the encryption computation **(paragraph 90, Yamamichi teaches the decrypting unit performing the decryption which is the inverse of the encryption that was used.)**, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages **(paragraphs 90-92, Yamamichi teaches the decryption unit decrypting the encrypted message. Yamamichi, paragraph 14, also teaches decrypting the multiple(n) encrypted messages to obtain multiple(n) decrypted messages.)**, and a number of decrypted messages generated by the decryption unit being equal to the number of encrypted messages generated from the one message by the encryption unit **(paragraphs 11-14, Yamamichi teaches encrypted a message n times to generate n encrypted messages. Yamamichi also teaches decrypting the n encrypted messages n times to generate n decrypted messages. Therefore, the number of decrypted messages is equal to the number of encrypted messages.)**; a computation unit operable to perform the one-way

operation on the decrypted message to generate a decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit **(paragraphs 97-98, Yamamichi teaches the one-way operation unit performing a one-way operation (hash) on the decrypted information and generating a functional value.)**; and a judging unit operable to compare each of the decryption computation values with the received comparison computation value **(paragraphs 100-101, Yamamichi teaches comparing the original plaintext message hash value with the decrypted messages hash value to determine if there was a decryption error or not.)**, wherein (i) when at least one of the decryption computation values matches the received comparison computation value **(paragraphs 119-112, Yamamichi teaches a comparison unit that compares the decrypted hash values with the original hash values to determine if a decryption error has occurred or not. If the two hash values match then a decryption error has not occurred.)** determining that a decryption error did not occur **(paragraphs 119-112, Yamamichi teaches a comparison unit that compares the decrypted hash values with the original hash values to determine if a decryption error has occurred or not. If the two hash values match then a decryption error has not occurred.)**, and (ii) when none of the decryption computation values matches the received comparison computation value, the judging unit determines that there is a decryption error **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

However, Yamamichi does not specifically disclose performing the one-way operation on multiple decrypted messages to generate multiple decryption computation values.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the invention of Yamamichi perform multiple one-way operations. Yamamichi, paragraphs 11-16, teaches performing multiple encryptions on the same plaintext message to generate multiple encrypted messages. These messages are then decrypted to form a plurality of decrypted messages. These decrypted messages are then compared to determine if there was a decryption error has occurred. Yamamichi, paragraphs 100-101, also teach performing the one-way operation on the original plaintext message and also on the decrypted message to generate two hash values. These two hash values are then compared to determine if there was a decryption error. The examiner feels that if multiple encryptions/decryptions can be performed and compared to determine if a decryption error has occurred, and a hash function can also be used to determine if a decryption error has occurred, then it would be obvious to perform the hash function multiple times on the decrypted messages and compare each hash value to the original plaintext messages hash value to determine if a decryption error has occurred or not.

Yamamichi also does not specifically disclose outputting the decrypted message if it is determined that a decryption error did not occur.

Olson discloses the judging unit outputs decrypted message as a correct decrypted message **(paragraph 52, Olsen teaches outputting the decrypted**

message if the decryption was successful or outputting an error message if the decryption was not successful.)

Yamamichi and Olson are analogous are because they are from the same field of endeavor of message encryption and decryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Yamamichi by adding the teachings of Olson because it would allow a user to actually view the decrypted message that was sent. Otherwise the user would know that the message was received and decrypted correctly, but not what the message was.

As per claim 2, Yamamichi in view of Olson discloses the encryption communication system of Claim 1 **[See rejection to claim 1 above]**, wherein the encryption computation used by the encryption unit conforms to NTRU cryptosystem **(paragraph 77, Yamamichi teaches using the NTRU encryption cryptosystem to encrypt the data.)**, and wherein the decryption computation used by the decryption unit conforms to the NTRU cryptosystem **(paragraph 90, Yamamichi teaches decrypting using the inverse of the encryption algorithm which would have to be the NTRU decryption cryptosystem.)**

As per claim 7, Yamamichi discloses an encryption reception apparatus for secret message communication with an encryption transmission apparatus **(paragraph 27, Yamamichi teaches having a transmission apparatus and reception apparatus in order to encrypt and send data.)**, the encryption transmission apparatus storing

one message **(paragraph 56, Yamamichi teaches having plaintext storage to store the message to be encrypted.)**, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple encrypted messages from the single plaintext message(m).)**, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one mesasage **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**, performing a one-way operation on the one message to generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the plaintext message to calculate a value.)**, and transmitting **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of

encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple encrypted messages.)**, the encryption reception apparatus comprising: a reception unit operable to receive **(paragraph 84, Yamamichi teaches having the receiving unit receive data.)**, from the encryption transmission apparatus **(paragraph 84, Yamamichi teaches having the receiving unit receive the data from the transmission apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 84, Yamamichi teaches having the receiving unit receive the ciphertext and the hash value. Yamamichi, paragraph 14, also teaches the reception of the multiple encrypted messages.)**; a decryption unit operable to perform a decryption computation **(paragraphs 85- 90, Yamamichi teaches having a decrypting unit to decrypt the encrypted data.)**, corresponding to the encryption computation **(paragraph 90, Yamamichi teaches the decrypting unit performing the decryption which is the inverse of the encryption that was used.)**, the decryption computation being performed on each of the encrypted messages to generate a plurality decrypted messages **(paragraphs 90-92, Yamamichi teaches the decryption unit decrypting the encrypted message. Yamamichi, paragraph 14, also teaches decrypting the multiple(n) encrypted messages to obtain multiple(n) decrypted messages.)**, and a number of decrypted messages generated by the decryption unit being equal to the number of encrypted messages generated from the one message by the encryption transmission apparatus **(paragraphs 11-14,**

Yamamichi teaches encrypted a message n times to generate n encrypted messages. Yamamichi also teaches decrypting the n encrypted messages n times to generate n decrypted messages. Therefore, the number of decrypted messages is equal to the number of encrypted messages.); a computation unit operable to perform the one-way operation on the decrypted message to generate a decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit **(paragraphs 97-98, Yamamichi teaches the one-way operation unit performing a one-way operation (hash) on the decrypted information and generating a functional value.)**; and a judging unit operable to compare each of the decryption computation values with the received comparison computation value **(paragraphs 100-101, Yamamichi teaches comparing the original plaintext message hash value with the decrypted messages hash value to determine if there was a decryption error or not.)**, wherein (i) when at least one of the decryption computation values matches the received comparison computation value **(paragraphs 119-112, Yamamichi teaches a comparison unit that compares the decrypted hash values with the original hash values to determine if a decryption error has occurred or not. If the two hash values match then a decryption error has not occurred.)** determining that a decryption error did not occur **(paragraphs 119-112, Yamamichi teaches a comparison unit that compares the decrypted hash values with the original hash values to determine if a decryption error has occurred or not. If the two hash values match then a decryption error has not occurred.)**, and

(ii) when none of the decryption computation values matches the received comparison computation value, the judging unit determines that there is a decryption error **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

However, Yamamichi does not specifically disclose performing the one-way operation on multiple decrypted messages to generate multiple decryption computation values.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the invention of Yamamichi perform multiple one-way operations. Yamamichi, paragraphs 11-16, teaches performing multiple encryptions on the same plaintext message to generate multiple encrypted messages. These messages are then decrypted to form a plurality of decrypted messages. These decrypted messages are then compared to determine if there was a decryption error has occurred. Yamamichi, paragraphs 100-101, also teach performing the one-way operation on the original plaintext message and also on the decrypted message to generate two hash values. These two hash values are then compared to determine if there was a decryption error. The examiner feels that if multiple encryptions/decryptions can be performed and compared to determine if a decryption error has occurred, and a hash function can also be used to determine if a decryption error has occurred, then it would be obvious to perform the hash function multiple times on the decrypted messages and compare each

hash value to the original plaintext messages hash value to determine if a decryption error has occurred or not.

Yamamichi also does not specifically disclose outputting the decrypted message if it is determined that a decryption error did not occur.

Olson discloses the judging unit outputs decrypted message as a correct decrypted message **(paragraph 52, Olsen teaches outputting the decrypted message if the decryption was successful or outputting an error message if the decryption was not successful.)**

Yamamichi and Olson are analogous are because they are from the same field of endeavor of message encryption and decryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Yamamichi by adding the teachings of Olson because it would allow a user to actually view the decrypted message that was sent. Otherwise the user would know that the message was received and decrypted correctly, but not what the message was.

As per claim 8, Yamamichi in view of Olson discloses the encryption reception apparatus of Claim 7 **[See rejection to claim 7 above]**, wherein the encryption transmission apparatus performs an invertible data conversion on the one message to generate a converted message, performs an encryption algorithm on the converted message to generate one encrypted message **(paragraphs 71-79, Yamamichi teaches the function of the encrypting unit. Yamamichi teaches generating a random number and using that generated random number along with a key to**

encrypt data. Yamamichi also teaches adding the random number to the data, which is invertible, and then encrypting the data.), and repeats the generation of the converted message and the generation of the one encrypted message **(paragraph 11, Yamamichi teaches generating multiple random numbers and then encrypting the same message(m) multiple(n) times using the random numbers and a key to generate multiple encrypted messages.)**, the generation of the converted one message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one message to generate the plurality of encrypted messages **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**, and wherein the decryption unit comprises: a decryption computation subunit operable to perform a decryption algorithm corresponding to the encryption algorithm **(paragraph 90, Yamamichi teaches the decrypting unit performing a decryption which is the inverse of the encryption that was used.)**, on one of the plurality of the encrypted messages to generate one decrypted text **(paragraph 14, Yamamichi teaches the decryption of the multiple messages. Each encrypted message is decrypted to form a decrypted message. For example, encrypted message c_1 is decrypted to form decrypted message m'_1.)**, and perform an inverse conversion of the invertible data conversion on the one decrypted text to

generate one decrypted message **(paragraph 95, Yamamichi discloses the information removing unit removing the random number from the decrypted data, which is the inverse of adding the random number that the encrypting unit performs.)**; and a repetition control subunit operable to control the decryption computation subunit to repeat the generation of the one decrypted content and the generation of the one decrypted message **(paragraph 14, Yamamichi teaches the decrypting of the multiple decrypted messages.)**, the generation of the one decrypted content and the generation of the one decrypted message being repeated the plural number of times the decryption unit performs the decryption computation to generate the plurality of the decrypted messages being equal in number to the number of encrypted messages generated from the one message by the encryption unit **(paragraphs 11-15, Yamamichi teaches encrypting/decrypting messages. One plaintext message is encrypted n times to generate n encrypted messages. Those n encrypted messages are then decrypted to form n decrypted messages. Therefore, the number of decrypted messages is equal to the number of encrypted messages and the number is n.)**

As per claim 9, Yamamichi in view of Olson discloses the encryption reception apparatus of Claim 8 **[See rejection to claim 8 above]**, wherein the encryption transmission apparatus generates a random number of a fixed length, and generates the converted message by adding the random number to the one message **(paragraphs 70-79, Yamamichi teaches the transmission apparatus generating a random number and adding that number to the data to be encrypted, by the**

information adding unit.), and wherein the decryption computation subunit generates the one decrypted message by removing the random number of the fixed length from the one decrypted text **(paragraph 95, Yamamichi teaches the reception apparatus having the information removing unit remove the random number from the decrypted content.)**

As per claim 10, Yamamichi in view of Olson discloses the encryption reception apparatus of Claim 9 **[See rejection to claim 9 above]**, wherein the encryption algorithm used by the encryption transmission apparatus conforms to NTRU cryptosystem **(paragraph 77, Yamamichi teaches the use of the NTRU encryption cryptosystem.)**, and wherein the decryption algorithm used by the decryption computation subunit conforms to the NTRU cryptosystem **(paragraph 90, Yamamichi teaches decrypting using the inverse of the encryption algorithm which would have to be the NTRU decryption cryptosystem.)**

As per claim 14, Yamamichi discloses an encryption reception method used in an encryption reception apparatus the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted data from the transmission unit.)**, the encryption transmission apparatus storing one message **(paragraph 58, Yamamichi teaches the transmission apparatus having a plaintext storage to store the message to be encrypted.)**, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages

from the one message **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple encrypted messages from the one plaintext message.)**, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one message **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**, performing a one-way operation on the one message to generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and transmitting **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple**

encrypted messages.), the encryption reception method comprising: receiving **(paragraph 84, Yamamichi teaches having a receiving unit to receive the encrypted data.)**, from the encryption transmission apparatus **(paragraph 84, Yamamichi teaches the receiving unit receiving data from the transmission apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted message and the hash value from the transmission apparatus. Yamamichi, paragraph 14, also teaches the reception of the multiple encrypted messages.)**; performing a decryption computation corresponding to the encryption computation **(paragraph 90, Yamamichi teaches the decrypting unit performing the decryption which is the inverse of the encryption that was used.)**, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages **(paragraphs 90-92, Yamamichi teaches the decryption unit decrypting the encrypted message. Yamamichi, paragraph 14, also teaches decrypting the multiple(n) encrypted messages to obtain multiple(n) decrypted messages.)**, and a number of decrypted messages generated by the performing of the decryption computation being equal to the number of encrypted messages generated from the one message by the encryption transmission apparatus **(paragraphs 11-14, Yamamichi teaches encrypted a message n times to generate n encrypted messages. Yamamichi also teaches decrypting the n encrypted messages n times to generate n decrypted messages. Therefore, the number of decrypted messages is equal to the number of encrypted messages.)**; performing

the one-way operation on the decrypted message to generate a decryption computation value, a number of decryption computation values generated by the performing of the one-way operation being equal to the number of the decrypted messages generated by the performing of the decryption computation **(paragraphs 97-98, Yamamichi teaches the one-way operation unit performing a one-way operation (hash) on the decrypted information and generating a functional value.)**; comparing each of the decryption computation values with the received comparison computation value **(paragraphs 100-101, Yamamichi teaches comparing the original plaintext message hash value with the decrypted messages hash value to determine if there was a decryption error or not.)**; outputting a value, based on the comparing when the decryption computation value matches the received comparison computation value **(paragraphs 119-112, Yamamichi teaches a comparison unit that compares the decrypted hash values with the original hash values to determine if a decryption error has occurred or not. If the two hash values match then a decryption error has not occurred.)**, and determining that there is a decryption error when, as a result of the comparing, the decryption computation values does not match the received comparison computation value **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

However, Yamamichi does not specifically disclose performing the one-way operation on multiple decrypted messages to generate multiple decryption computation values.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the invention of Yamamichi perform multiple one-way operations. Yamamichi, paragraphs 11-16, teaches performing multiple encryptions on the same plaintext message to generate multiple encrypted messages. These messages are then decrypted to form a plurality of decrypted messages. These decrypted messages are then compared to determine if there was a decryption error has occurred. Yamamichi, paragraphs 100-101, also teach performing the one-way operation on the original plaintext message and also on the decrypted message to generate two hash values. These two hash values are then compared to determine if there was a decryption error. The examiner feels that if multiple encryptions/decryptions can be performed and compared to determine if a decryption error has occurred, and a hash function can also be used to determine if a decryption error has occurred, then it would be obvious to perform the hash function multiple times on the decrypted messages and compare each hash value to the original plaintext messages hash value to determine if a decryption error has occurred or not.

Yamamichi also does not specifically disclose outputting the decrypted message if it is determined that a decryption error did not occur.

Olson discloses the judging unit outputs decrypted message as a correct decrypted message **(paragraph 52, Olsen teaches outputting the decrypted message if the decryption was successful or outputting an error message if the decryption was not successful.)**

Yamamichi and Olson are analogous are because they are from the same field of endeavor of message encryption and decryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Yamamichi by adding the teachings of Olson because it would allow a user to actually view the decrypted message that was sent. Otherwise the user would know that the message was received and decrypted correctly, but not what the message was.

As per claim 15, Yamamichi discloses a computer-readable recording medium having an encryption reception program recorded thereon, the encryption reception program being used in an encryption reception apparatus **(paragraph 82, Yamamichi teaches the reception apparatus having a computer program.)**, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted data from the transmission unit.)**, the encryption transmission apparatus storing one message **(paragraph 58, Yamamichi teaches the transmission apparatus having a plaintext storage to store the message to be encrypted.)**, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple**

encrypted messages from the one plaintext message.), a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one message **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**, performing a one-way operation on the one message to generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and transmitting **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple encrypted messages.)**, the encryption reception program comprising: receiving **(paragraph 84, Yamamichi teaches having a receiving unit to receive the encrypted data.)**, from the encryption transmission apparatus **(paragraph 84, Yamamichi teaches the receiving unit**

receiving data from the transmission apparatus.), the plurality of the encrypted messages and the comparison computation value **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted message and the hash value from the transmission apparatus. Yamamichi, paragraph 14, also teaches the reception of the multiple encrypted messages.)**; performing a decryption computation corresponding to the encryption computation **(paragraph 90, Yamamichi teaches the decrypting unit performing the decryption which is the inverse of the encryption that was used.)**, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages **(paragraphs 90-92, Yamamichi teaches the decryption unit decrypting the encrypted message. Yamamichi, paragraph 14, also teaches decrypting the multiple(n) encrypted messages to obtain multiple(n) decrypted messages.)**, and a number of decrypted messages generated by the performing of the decryption computation being equal to the number of encrypted messages generated from the one message by the encryption transmission apparatus **(paragraphs 11-14, Yamamichi teaches encrypted a message n times to generate n encrypted messages. Yamamichi also teaches decrypting the n encrypted messages n times to generate n decrypted messages. Therefore, the number of decrypted messages is equal to the number of encrypted messages.)**; performing the one-way operation on the decrypted message to generate a decryption computation value, a number of decrypted computation values generated by the performing of the one-way operation being equal to the number of the decrypted messages generated by the performing of the decryption computation

(paragraphs 97-98, Yamamichi teaches the one-way operation unit performing a one-way operation (hash) on the decrypted information and generating a functional value.); comparing each of the decryption computation values with the received comparison computation value **(paragraphs 100-101, Yamamichi teaches comparing the original plaintext message hash value with the decrypted messages hash value to determine if there was a decryption error or not.)**; outputting a value, based on the comparing when the decryption computation value matches the received comparison computation value **(paragraphs 119-112, Yamamichi teaches a comparison unit that compares the decrypted hash values with the original hash values to determine if a decryption error has occurred or not. If the two hash values match then a decryption error has not occurred.)**, and determining that there is a decryption error when, as a result of the comparing, the decryption computation values does not match the received comparison computation value **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

However, Yamamichi does not specifically disclose performing the one-way operation on multiple decrypted messages to generate multiple decryption computation values.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the invention of Yamamichi perform multiple one-way operations. Yamamichi, paragraphs 11-16, teaches performing multiple encryptions on the same

plaintext message to generate multiple encrypted messages. These messages are then decrypted to form a plurality of decrypted messages. These decrypted messages are then compared to determine if there was a decryption error has occurred. Yamamichi, paragraphs 100-101, also teach performing the one-way operation on the original plaintext message and also on the decrypted message to generate two hash values. These two hash values are then compared to determine if there was a decryption error. The examiner feels that if multiple encryptions/decryptions can be performed and compared to determine if a decryption error has occurred, and a hash function can also be used to determine if a decryption error has occurred, then it would be obvious to perform the hash function multiple times on the decrypted messages and compare each hash value to the original plaintext messages hash value to determine if a decryption error has occurred or not.

Yamamichi also does not specifically disclose outputting the decrypted message if it is determined that a decryption error did not occur.

Olson discloses the judging unit outputs decrypted message as a correct decrypted message **(paragraph 52, Olsen teaches outputting the decrypted message if the decryption was successful or outputting an error message if the decryption was not successful.)**

Yamamichi and Olson are analogous are because they are from the same field of endeavor of message encryption and decryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Yamamichi by adding the teachings of Olson

because it would allow a user to actually view the decrypted message that was sent. Otherwise the user would know that the message was received and decrypted correctly, but not what the message was.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. **Claims 3-6 and 11-12** are rejected under 35 U.S.C. 102(b) as being anticipated by Yamamichi.

As per claim 3, Yamamichi discloses an encryption transmission apparatus for secret message communication with an encryption reception apparatus **(paragraph 27, Yamamichi teaches having a transmission apparatus and reception apparatus in order to encrypt data.)**, the encryption transmission apparatus comprising: a storage unit that stores one message **(paragraph 56, Yamamichi teaches having plaintext storage to store the message to be encrypted.)**; an encryption unit operable to perform an encryption computation on the message a plural number of times to generate a plurality of encrypted messages from the one message **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple**

encrypted messages.), a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message **(paragraphs 11-14, Yamamichi teaches encrypted a message n times to generate n encrypted messages. Yamamichi also teaches decrypting the n encrypted messages n times to generate n decrypted messages. Therefore, the number of decrypted messages is equal to the number of encrypted messages.)**; a computation unit operable to perform a one-way operation on the one message **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; to generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and a transmission unit operable to transmit **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple encrypted messages.)**

As per claim 4, Yamamichi discloses the encryption transmission apparatus of Claim 3 **[See rejection to claim 3 above]**, wherein the encryption unit comprises: an

encryption computation subunit operable to perform an invertible data conversion on the one message to generate a converted message, and perform an encryption algorithm on the converted message to generate one encrypted message **(paragraphs 71-79, Yamamichi teaches the function of the encrypting unit. Yamamichi teaches generating a random number and using that generated random number along with a key to encrypt data. Yamamichi also teaches adding the random number to the data, which is invertible, and then encrypting the data.)**; and a repetition control subunit operable to control the encryption computation subunit to repeat the generation of the converted message and the generation of the one encrypted message **(paragraph 11, Yamamichi teaches generating multiple random numbers and then encrypting the same message(m) multiple(n) times using the random numbers and a key to generate multiple encrypted messages.)**, the generation of the converted message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one message to generate the plurality of encrypted messages **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**

As per claim 5, Yamamichi discloses the encryption transmission apparatus of Claim 4 **[See rejection to claim 4 above]**, wherein the encryption computation subunit

generates a random number of a fixed length, and generates the converted message by adding the random number to the one message **(paragraphs 70-79, Yamamichi teaches generating a random number and adding that number, to the data to be encrypted, by the information adding unit.)**

As per claim 6, Yamamichi discloses the encryption transmission apparatus of Claim 5 **[See rejection to claim 5 above]**, wherein the encryption algorithm used by the encryption computation subunit on the converted message conforms to NTRU cryptosystem **(paragraph 77, Yamamichi teaches the use of the NTRU encryption cryptosystem.)**

As per claim 11, Yamamichi discloses an encryption transmission method used in an encryption transmission apparatus, the encryption transmission apparatus storing one message and transmitting the one message in secrecy to an encryption reception apparatus **(paragraph 58, Yamamichi teaches having storage to store a plaintext message. In paragraph 81, Yamamichi also discloses the transmission apparatus having a transmitting unit to transmit the encrypted or secret data.)**, the encryption transmission method comprising: performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple encrypted messages from the one plaintext**

message.), a number of encrypted messages generated from the one message by the performing of the encryption computation being equal to the number of times the performing of the encryption computation performs the encryption computation on the one message **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**; performing a one-way operation on the one message to generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and transmitting **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple encrypted messages.)**

As per claim 12, Yamamichi discloses a computer-readable recording medium having an encryption transmission program recorded thereon, the encryption

transmission program being used in an encryption transmission apparatus **(paragraph 56, Yamamichi teaches having a computer program for the encryption transmission apparatus.)**, the encryption transmission apparatus storing one message and transmitting the message in secrecy to an encryption reception apparatus **(paragraph 58, Yamamichi teaches having storage to store a plaintext message. In paragraph 81, Yamamichi also discloses the transmission apparatus having a transmitting unit to transmit the encrypted or secret data.)**, the encryption transmission program causing the encryption transmission apparatus to execute a method comprising: performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform a single encryption. In paragraph 11, Yamamichi also discloses generating multiple random numbers and then encrypting the same message(m) multiple(n) times to generate multiple encrypted messages from the one plaintext message.)**, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal to the number of times the performing of the encryption performs the encryption computation on the one message **(paragraph 11, Yamamichi teaches encrypting the one message(m) multiple(n) times to generate multiple encrypted messages, c_1 through c_n. Yamamichi also teaches encrypting the message n times to generate n encrypted messages. N random numbers are generated and used to encrypt the single plaintext message n times to generate n encrypted messages.)**; performing a one-way operation on the one message to

generate a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and transmitting **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value.)**, to the encryption reception apparatus **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the encrypted data and the hash value to the reception apparatus.)**, the plurality of the encrypted messages and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertext and the hash value to the reception apparatus. Yamamichi, paragraphs 13-14, also teaches the transmitting of the multiple encrypted messages.)**

Response to Arguments

10. The amendments to the specification are accepted as overcoming the objection for an embedded hyperlink of first Office Action, mailed September 30, 2008.

11. The amendments to the claims are accepted as overcoming the rejections under 35 U.S.C. 112, second paragraph of the first Office Action, mailed September 30, 2008.

12. Applicant's arguments filed 28 October 2008 have been fully considered but they are not persuasive. In the remarks applicant argues that the cited prior art does not cover the following limitations:

I) encrypting one message a plural number of times to generate a plural number of encrypted messages where the number of encrypted messages is equal to the number of encryptions performed

II) decrypting each of the plurality of encrypted messages to generate a plurality of decrypted messages where the number of decrypted messages is equal to the number of decrypted messages which is also equal to the number of encrypted messages and encryptions performed.

III) determining if a decryption error has occurred and outputting the decrypted message if no error has occurred

In response to applicant's arguments:

I) The examiner agrees that Yamamichi's claimed invention does not teach encrypting the one message a plural number of times. However, Yamamichi does disclose the specifics of the NTRU cryptosystem in paragraphs 11-14 of the background, which discusses encrypting a single plaintext message multiple times to generate multiple encrypted messages. The encryption is performed n times and generates n encrypted messages. Therefore, Yamamichi does teach the required limitation.

II) The examiner agrees that Yamamichi's claimed invention does not teach decrypted multiple messages. However, Yamamichi does disclose the specifics of the NTRU cryptosystem in paragraphs 11-14 of the background, which discusses decrypting each encrypted message to generate a plurality of decrypted messages. The decryption is performed n times to generate n decrypted messages, which is also the same number of encryptions and encrypted messages. Therefore, Yamamichi does teach the required limitation.

III) The argument is considered moot based upon the new grounds of rejection above.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN B. KING whose telephone number is (571)270-7310. The examiner can normally be reached on Mon. - Thur. 7:30 AM - 5:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JBK

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148